



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|-------------------------|------------------|
| 09/827,226 | 04/05/2001 | Marcus Wong | 1 | 6211 |
| 7590 | 08/07/2006 | | EXAMINER | |
| David J. Gaskey Carison, Gaskey & Olds, PC 400 West Maple Road Suite #350 Birmingham, MI 48009 | | | SHIFERAW, ELENI A | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2136 | |
| | | | DATE MAILED: 08/07/2006 | |

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|------------------------------|------------------------|---------------------|--|
| | 09/827,226 | WONG, MARCUS | |
| | Examiner | Art Unit | |
| | Eleni A. Shiferaw | 2136 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 25 April 2006.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 21-40 is/are pending in the application.
4a) Of the above claim(s) 1-20 is/are withdrawn from consideration.
5) Claim(s) _____ is/are allowed.
6) Claim(s) 21-40 is/are rejected.
7) Claim(s) _____ is/are objected to.
8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .

5) Notice of Informal Patent Application (PTO-152)

6) Other: ____ .

DETAILED ACTION

Response to Amendment

1. Applicant's arguments and amendments with respect to canceled claims 1-20 and newly added claims 21-40 and presently pending claims 21-40, filed on 04/25/2006 have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

Response to Arguments

2. Applicant cancels all the claims 1-20 and adds all new claims 21-40, and argues the double rejection under 102 b of **Hwang references** are *not anticipated because Hwang references use random number as a value allegedly corresponding to the common key value of Applicant's claims. A random number is not a function of a session key or any portion of a session key*, Remark page 7. However the Examiner disagrees with the Applicant's contention and would like to draw the Applicant's attention to page 1470 section II A wherein Hwang discloses the steps of distributing common key. Yes, as applicant agreed the common keys (CK) generated by Network center are provided to terminals (Ti). CK is generated from random numbers r11 and r12 chosen, such that $r1 = r11 + r12$. However, the random number is not just a random number as the applicant argues. The random number is the session key-decryption key (see, Hwang '99 page 1470 section II A steps 1 and 4). Therefore CK is generated as a function of at least a portion of at least one of the first session key or the second key. Accordingly the rejection for claims 21-40 are maintained.

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 21-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Hwang (IEEE '99, Dynamic Participation in a Secure Conference Scheme for Mobile communications).

Regarding claims 21 and 33 Hwang discloses a method of providing secure communications between a first wireless unit that uses a first session key and a second wireless unit that uses a second session key, the method comprising:

generating a common key value as a function of at least a portion of at least one of first session key or the second session key (page 1470 section II A steps 1 and 4; *random number r11 and r12 is a session key-decryption key*);

providing/receiving the common key value to the first wireless unit (page 1471 col. 1 lines 17-24; *trusted network center (NC) generating and providing common key to the first wireless terminal (T1)*) for use in secure communications between the first wireless unit and the second wireless unit having the common key value (page 1471 col. 1 lines 19-20 and page 1469 section I paragraph 3; *any participant (second or third terminals) gets common key, for secure mobile communications without the communication unit involving to encrypt/decrypt message exchanged between the terminals*).

Regarding claim 22, Hwang discloses the method comprising:

sending the common key value to the first wireless unit using the first session key (see, fig. 1 element g; *common key is sent to Ti that is generated based on terminal 1 => r11 and r12 session key-decryption key*).

Regarding claim 23, Hwang teaches the method comprising

sending the common key value to the second wireless unit using the second session key (see, fig. 1 element g; *common key is sent to Ti that is generated based on terminal 2 => r11 and r12 session key-decryption key*).

Regarding claim 24, Hwang discloses the method comprising

encrypting the common key value with the second session key (page 1470 steps 7-9; *common key is encrypted using NC's key*); and
transmitting the encrypted common key value to the second wireless unit (page 1470-1471 section II; *encrypted CK is transmitted to Ti*).

Regarding claim 25, Hwang teaches the method comprising

encrypting the common key value using the first session key (page 1470 steps 7-9; *common key is encrypted using NC's key according to next terminal*); and
transmitting the encrypted common key value to the first wireless unit (page 1470 steps 7-9; *transmitting encrypted common key to Ti*).

Regarding claim 26, Hwang discloses the method comprising

generating the first session key as a function of a first root key known only at the first wireless unit and a wireless communication system accessed by at least the first wireless unit (see page 1470 section II A step 4; *each terminal generating random number as a session key-decryption key*).

Regarding claim 27, Hwang discloses the method comprising

generating the second session key as a function of a second root key known only at said second wireless unit and at a home wireless communication system accessed by at least said second wireless unit (page 1470 section A steps 1-7; *Network center generating common secret session key CK for each participant terminals based on random number each terminal generate*).

Regarding claims 28 and 39, Hwang discloses the method comprising

generating the common key value as a function of the first session key and the second session key (page 1470 section A steps 1-7; *Network center generating common secret session key CK for each participant terminals based on session key-decryption key*).

Regarding claim 29, Hwang discloses the method comprising

generating the common key value as an encryption key (abstract; *CK for encryption*).

Regarding claim 30, Hwang teaches the method comprising

generating the common key value as a session key (page 1471lines 19-20; *CK, common secret session key*).

Regarding claim 31, the method comprising

mutually generating the common key value by a first wireless communicating system accessed by the first wireless unit and a second wireless communication system accessed by the second wireless unit (page 1470 fig. 1).

Regarding claims 32 and 40, Hwang teaches the method comprising

using the common key value for a first communication session between the first and second wireless units (pages 1470-1471 section I); and

using the same communication key value for a second, different communication session between the first and second wireless units (pages 1470-1471 section I).

Regarding claim 34, Hwang teaches the method comprising

generating the first session key corresponding to the first wireless unit (page 1470 section II; *terminal-1 with key e (AK1) (r11 and r12 session key-decryption key) ...that is used to request session key from network center, and Applicant Admitted Prior Art (AAPA) explains root key/A_key/AK1, on page 3-5, as a well-known*); and

obtaining the common key value by the first wireless unit using the first session key (Hwang page 1470 steps 7-9; $CK=(Q \cdot 2^2 + R) \bmod ri$).

Regarding claim 35, Hwang discloses the method comprising

decrypting the common key value using the first session key (page 1470 steps 4-7).

Regarding claim 36, Hwang discloses the method wherein

the first session key is generated as a function of a first root key known only at the first wireless unit and a wireless communication system accessed by at least the first wireless unit (page 1470 section A steps 1-7; *Network center generating common secret session key CK for each participant terminals based on random number each terminal generate*).

Regarding claim 37, Hwang discloses the method comprising

using the common key as an encryption key (abstract; *CK for encryption*).

Regarding claim 38, Hwang discloses the method comprising

using the common key as a session key (page 1471lines 19-20; *CK, common secret session key*).

5. Claims 21 and 33 are also rejected under 35 U.S.C. 102(b) as being anticipated by Hwang '92, (IEEE 1992, Scheme for secure digital mobile communications based on symmetric key Cryptography).

Regarding claims 21 and 33, Hwang '92 discloses a method of providing secure communications between a first wireless unit and a second wireless unit that uses a second session key, said method comprising the step of:

generating a common key value as a function of at least a portion of at least one of the first session key or the second session key and receiving at the first wireless unit, a common key value (page 423 section II; *generating a common key based on nonce*); and

providing a common key value to a first wireless unit for use in secure communications over at least one wireless communications system between said first wireless unit and said second wireless unit having said common key (page 423 section II; *network center provides session symmetric key & nonce to the mobile unit-1...mobile unit-1 decrypts the encrypted session symmetric key & nonce and compares the nonce unit-1 sent with received and if match, unit-1 encrypts the message using symmetric session key and sends the encrypted message & unit-2 nonce to mobile user-2.... unit-2 authenticates the nonce same as unit-1 and decrypts the encrypted message sent from user-1 using symmetric session key and mobile unit-1 and unit-2 are securely communicated without the network center encrypting and decrypting messages exchanged between the units and/or no significant amount of processing by the network center is required to encrypt/decrypt data sent between the first and second mobile units*).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.



02/18/2006